JP10022994A CIPHERING DEVICE, DECIPHERING DEVICE, CIPHERING METHOD, DECIPHERING METHOD AND COMMUNICATION SYSTEM USING THE SAME

Bibliography

DWPI Title

Encipherment apparatus used in communication systems, portable telephone has encrypted key generation part that forms encrypted key based on information setup for every connection of communication circuit between main station and mobile station

Original Title

CIPHERING DEVICE, DECIPHERING DEVICE, CIPHERING METHOD, DECIPHERING METHOD AND COMMUNICATION SYSTEM USING THE SAME

Assignee/Applicant

Standardized: HITACHI LTD
Original: HITACHI LTD

Inventor

KOIDE AYUMI ; TAKARAGI KAZUO

Publication Date (Kind Code)

1998-01-23 (A)

Application Number / Date

JP1996175043A / 1996-07-04

Priority Number / Date / Country

JP1996175043A / 1996-07-04 / JP

Abstract

PROBLEM TO BE SOLVED: To make decoding difficult and to securely synchronize passwords by generating a password key based on information which is set at every connection of a communication line between a base station and a moving station.

SOLUTION: Ciphering is executed by using the key generated in a key generation part 200. The key generation part generates the password key based on information or the like which are set every time when the communication line is connected between the base station and the moving station. The password keys taking dynamic values different in every communication connection or every arbitrary time are made by generating the key from information. Random numbers outputted from a random number generation circuit part 202 are fed back and used as initial values for generating the next random numbers. The generated random numbers and data to be transmitted are operated in an exclusive OR operation part 203 and a password sentence of generated.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－22994

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ	9/20			Ｈ０４Ｌ	9/00	６５３
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ｄ
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｒ
Ｈ０４Ｌ	9/12			Ｈ０４Ｌ	9/00	６３１
	9/16					６４３

審査請求　未請求　請求項の数25　ＯＬ　（全 15 頁）

(21)出願番号　特願平8－175043

(22)出願日　平成８年(1996)７月４日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　小出　歩
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所情報通信事業部内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　高橋　明夫　（外１名）

(54)【発明の名称】　暗号化装置および復号化装置、暗号化方法および復号化方法、ならびにそれらを用いた通信システム

(57)【要約】

【課題】暗号化装置および復号化装置において、従来より、より解読を困難にしつつ暗号同期が確実にとれるようにする。

【解決手段】暗号化装置と復号化装置とに、暗号鍵を生成する暗号鍵生成部と、初期入力値を格納するレジスタと、暗号鍵生成部で生成した暗号鍵とレジスタに格納された初期入力値を入力し、予め定められた演算処理を行い乱数を生成し出力する乱数生成回路と、その乱数を用いて伝送しようとする入力データに暗号化を施す演算部を設け、暗号鍵生成部は、通信回線を接続する度に設定される情報に基づいて暗号鍵を生成するようにし、さきの初期入力値に予め定められた演算処理を施して次の乱数を生成するための乱数生成回路の初期入力値とする初期値演算処理部とを設ける。

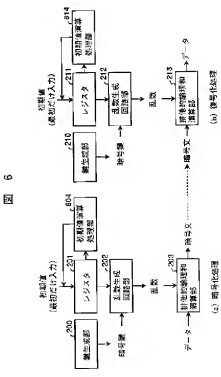


図６

【特許請求の範囲】
【請求項１】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムに係り、秘匿性を要する伝送データの暗号化に用いられる暗号化装置において、
この暗号化装置は、
暗号鍵を生成する暗号鍵生成部と、
初期入力値を格納するレジスタと、
前記暗号鍵生成部で生成した暗号鍵と前記レジスタに格納された初期入力値を入力し、予め定められた演算処理を行い乱数を生成し出力する乱数生成回路と、
前記伝送データに対し、前記乱数を用いて暗号化を施す演算部とを有し、
前記暗号鍵生成部は、前記基地局と前記移動局との間の通信回線の接続ごとに設定される情報に基づいて暗号鍵を生成することを特徴とする暗号化装置。
【請求項２】　請求項１記載の暗号化装置において、
前記暗号鍵生成部は、
通信回線の接続ごとに設定される情報として、前記基地局の基地局識別情報、前記移動局の移動局識別情報、前記基地局と前記移動局の通信接続情報、前記移動局の移動局認識情報、通信接続に関連する時間情報、前記移動局の位置情報のうちの一つまたは複数を用い、
予め定められた演算規則に基づいて暗号化鍵を生成することを特徴とする暗号化装置。
【請求項３】　請求項１記載の暗号化装置において、
前記乱数生成回路は、予め定められた演算処理を行って生成した乱数列から、順々に乱数を生成する回路であって、
ある乱数を生成して、その生成された乱数を入力値として前記乱数生成回路は次の乱数を生成し、
その乱数を用いて前記演算部は前記伝送データに対し暗号化を施すことを特徴とする暗号化装置。
【請求項４】　請求項１記載の暗号化装置は、
前記乱数生成回路に入力された初期入力値に予め定められた演算処理を施す初期値演算処理部をさらに有し、
その演算処理を施した初期値を前記レジスタに格納し、
その前記レジスタに格納した演算処理を施した初期値を再びまた次の初期入力値として前記乱数生成回路は乱数を生成し、
その乱数を用いて前記演算部は前記伝送データに対し暗号化を施すことを特徴とする暗号化装置。
【請求項５】　請求項１記載の暗号化装置において、
前記通信システムによる通信は、フレームを伝送単位として行われ、
そのフレームのフレーム番号を前記レジスタに格納し、
そのレジスタに格納したフレーム番号を初期入力値として前記乱数生成回路は乱数を生成し、
その乱数を用いて前記演算部は前記伝送データに対し暗号化を施すことを特徴とする暗号化装置。
【請求項６】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムに係り、暗号化されて伝送されたデータの復号化に用いる復号化装置において、
この復号化装置は、
暗号鍵を生成する暗号鍵生成部と、
初期入力値を格納するレジスタと、
前記暗号鍵生成部で生成した暗号鍵と前記レジスタに格納された初期入力値を入力し、予め定められた演算処理を行い乱数を生成し出力する乱数生成回路と、
前記暗号化データを前記乱数を用いて復号化する演算部を有し、
前記暗号鍵生成部は、前記基地局と前記移動局との間の通信回線の接続ごとに設定される情報に基づいて暗号鍵を生成することを特徴とする復号化装置。
【請求項７】　請求項６記載の復号化装置において、
前記暗号鍵生成部は、通信回線の接続ごとに設定される情報として、前記基地局の基地局識別情報、前記移動局の移動局識別情報、前記基地局と前記移動局の通信接続情報、前記移動局の移動局認識情報、通信接続に関連する時間情報、前記移動局の位置情報のうちの一つまたは複数を用い、
予め定められた演算規則に基づいて暗号化鍵を生成することを特徴とする復号化装置。
【請求項８】　請求項６記載の復号化装置において、
前記乱数生成回路は、予め定められた演算処理を行って生成した乱数列から、順々に乱数を生成する回路であって、
ある乱数を生成して、その生成された乱数を入力値として前記乱数生成回路は次の乱数を生成し、
その乱数を用いて演算部は前記暗号化データを復号化することを特徴とする復号化装置。
【請求項９】　請求項６記載の復号化装置は、
前記乱数生成回路に入力された初期入力値に予め定められた演算処理を施す初期値演算処理部をさらに有し、
その演算処理を施した初期値を前記レジスタに格納し、
その演算処理を施した初期値を再びまた次の初期入力値として前記乱数生成回路は乱数を生成し、
その乱数を用いて前記演算部は前記暗号化データを復号化することを特徴とする復号化装置。
【請求項１０】　請求項６記載の復号化装置において、
前記通信システムによる通信は、フレームを伝送単位として行われ、
そのフレームのフレーム番号を前記レジスタに格納し、
そのレジスタに格納したフレーム番号を初期入力値として前記乱数生成回路は乱数を生成し、
その乱数を用いて前記演算部は前記暗号化データを復号することを特徴とする復号化装置。
【請求項１１】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムに係り、秘

匿性を要する伝送データの暗号化に用いられる暗号化方法において、
前記基地局と前記移動局との間の通信回線の接続ごとに設定される情報に基づいて暗号鍵を生成し、
その暗号鍵と初期入力値を用いて、予め定められた演算処理を行い乱数を生成し、
その乱数を用いて前記伝送データに対し暗号化を施すことを特徴とする暗号化方法。
【請求項１２】　請求項１１記載の暗号化方法において、
前記暗号鍵の生成は、通信回線の接続ごとに設定される情報として、前記基地局の基地局識別情報、前記移動局の移動局識別情報、前記基地局と前記移動局との通信接続情報、前記移動局の移動局認識情報、通信接続に関連する時間情報、前記移動局の位置情報のうちの一つまたは複数を用い、
予め定められた演算規則に基づいて暗号化鍵を生成することを特徴とする暗号化方法。
【請求項１３】　請求項１１記載の暗号化方法において、
前記乱数の生成は、予め定められた演算処理を行って生成した乱数列から順々に乱数を生成するものであって、ある乱数を生成して、その生成された乱数を入力値として、予め定められた演算処理を行い次の乱数を生成し、
その乱数を用いて前記伝送データに暗号化を施すことを特徴とする暗号化方法。
【請求項１４】　請求項１１記載の暗号化方法において、
前記初期入力値に予め定められた演算処理を施し、その演算処理を施した初期値を再びまた次の初期入力値として乱数を生成し、
その乱数を用いて前記伝送データに暗号化を施すことを特徴とする暗号化方法。
【請求項１５】　請求項１１記載の暗号化方法において、
前記通信システムによる通信は、フレームを伝送単位として行われ、
そのフレームのフレーム番号を初期入力値として乱数を生成し、
その乱数を用いて前記伝送データに対し暗号化を施すことを特徴とする暗号化方法。
【請求項１６】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムに係り、暗号化されて伝送されたデータの復号化に用いる復号化方法において、
前記基地局と前記移動局との間の通信回線の接続ごとに設定される情報に基づいて暗号鍵を生成し、
その暗号鍵と初期入力値を用いて予め定められた演算処理を行い乱数を生成し、
その乱数を用いて前記暗号化データを復号化することを特徴とする復号化方法。
【請求項１７】　請求項１６記載の復号化方法において、
前記暗号鍵の生成は、通信回線の接続ごとに設定される情報として、前記基地局の基地局識別情報、前記移動局の移動局識別情報、前記基地局と前記移動局の通信接続情報、前記移動局の移動局認識情報、通信接続に関連する時間情報、前記移動局の位置情報のうちの一つまたは複数を用い、
予め定められた演算規則に基づいて暗号化鍵を生成することを特徴とする復号化方法。
【請求項１８】　請求項１６記載の復号化方法において、
前記乱数の生成は、予め定められた演算処理を行って生成した乱数列から順々に乱数を生成するものであって、ある乱数を生成して、その生成された乱数を入力値として、予め定められた演算処理を行い次の乱数を生成し、
その乱数を用いて前記暗号化データを復号化することを特徴とする復号化方法。
【請求項１９】　請求項１６記載の復号化方法において、
前記初期入力値に予め定められた演算処理を施し、
その演算処理を施した初期値を再びまた次の初期入力値として乱数を生成し、
その乱数を用いて前記暗号化データを復号化することを特徴とする復号化方法。
【請求項２０】　請求項１６記載の復号化方法において、
前記通信システムによる通信は、フレームを伝送単位として行われ、
そのフレームのフレーム番号を初期入力値として乱数を生成し、
その乱数を用いて前記暗号化データを復号化を施すことを特徴とする復号化方法。
【請求項２１】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムにおいて、
前記基地局および前記移動局は、
請求項１記載の暗号化装置と、請求項６記載の復号化装置を有することを特徴とする通信システム。
【請求項２２】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムにおいて、
前記基地局および前記移動局は、
請求項３記載の暗号化装置と、請求項８記載の復号化装置を有することを特徴とする通信システム。
【請求項２３】　基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムにおいて、
前記基地局および前記移動局は、
請求項４記載の暗号化装置と、請求項９記載の復号化装置を有することを特徴とする通信システム。
【請求項２４】　基地局と、その基地局と通信回線を介

して通信を行う移動局を有する通信システムにおいて、
前記基地局および前記移動局は、
請求項５記載の暗号化装置と、請求項１０記載の復号化装置を有することを特徴とする通信システム。
【請求項２５】　請求項２２ないし２４記載の通信システムにおいて、
前記基地局と前記移動局との間のデータの伝送は制御情報領域と伝送情報領域を有する伝送スロットを介して行われ、
前記基地局および前記移動局は、
伝送する前記伝送スロットの制御情報領域が使用可能な状態であるかを判定する判定手段と、
前記制御情報領域に暗号同期情報をとるための暗号同期情報を書き込む手段と、
前記伝送スロットが暗号同期情報を伝送しているかどうかを示す暗号同期情報識別子を前記制御情報領域に付加する手段と、
受信した伝送スロットの制御情報領域の暗号同期情報識別子から前記伝送スロットが暗号同期情報を伝送しているかどうかを判定する手段と、
前記伝送スロットの制御情報領域から暗号同期情報を受け取る手段とをさらに有することを特徴とする通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、秘匿性を要するデータの暗号化装置および復号化装置、ならびに暗号化方法および復号化方法に係り、通信回線等を経由して情報の送受信を行う各種通信システムに利用され、特に暗号の解読が困難であり、しかも受信側と送信側の暗号同期をとるのが容易な暗号化装置および復号化装置、ならびに暗号化方法および復号化方法に関する。
【０００２】
【従来の技術】従来の暗号化装置および復号化装置について、図１および図１２を用いて説明をする。
【０００３】図１は、暗号化装置および復号化装置を利用した携帯電話システム全体の構成図である。
【０００４】図１に示すように、携帯電話システムは、複数の移動体端末１００～１０２と、複数の基地局１０３～１０５と、交換制御局１０６、および交換制御局１０６と固定電話網を介して接続された電話機等で構成される。暗号化装置および復号化装置１０９は、各移動体端末１００～１０２、および各基地局１０３～１０５に搭載されるものであり、音声符号化データやＦＡＸ、パソコン等の各種データの暗号化および復号化処理を行うものである。
【０００５】図１２（ａ）は、従来の通信システムに用いられている暗号化装置の構成と、データの流れを示した図である。
【０００６】図１２（ｂ）は、従来の通信システムに用いられている復号化装置の構成と、データの流れを示した図である。
【０００７】一般的に、通信システムにおいては、暗号化と復号化を行うための暗号鍵（キー）が同一である共通鍵暗号が使用されていた（共通鍵信号については、池野、小山著「現代暗号理論」電子情報通信学会参照）。その同一の鍵（共通鍵という）は、図示していないが、呼設定時に、送信側から受信側に送られ、送信者と受信者がそれぞれ所持する。送信側では、共通鍵を用いて暗号化したデータ（以下、暗号文という）を受信者に送り、受信者は、先に受け取った共通鍵を用いて復号化を行う。このようにして、特定の送受信者以外の第三者に解読されないようにデータの送受信を行っている。
【０００８】次に、暗号化装置および復号化装置の動作を説明する。
【０００９】図１２において、共通鍵、データ、暗号文は、それぞれ６４ビットを１単位として６４ビット毎に処理を行うものとする。
【００１０】従来の暗号化装置においては、まず、ある固定の共通鍵を、暗号化用の乱数生成回路部に入力する。図１２では、暗号化用の乱数生成回路部に、ＰＮ（PseudoNoise）パターン発生回路１２００を用いている。ＰＮパターン発生回路１２００は、入力された共通鍵に基づき、所定の演算アルゴリズムに従って乱数を生成する。排他的論理和演算部１２０５では、この乱数と暗号化しようとするデータとの排他的論理和をとることにより、暗号文を作成する。
【００１１】一方、復号化装置においては、送信側から送られてきた暗号文を受け取り、暗号化装置と同様の処理を行って乱数を生成し、暗号文と排他的論理和をとることにより、データを復号化する。
【００１２】従来、通信システムにおいて一般的に用いられている暗号化アルゴリズムは、上記のＰＮパターン発生回路を使った簡易的なものであった。
【００１３】また、ＰＮパターン発生回路などの乱数生成回路部へ入力する共通鍵は、暗号化するデータフレーム毎に、暗号化装置と復号化装置の両方で常に固定の値にリセットされる。ここで一フレームとは、数百ビットのデータをまとめた単位である。このリセットにより、暗号化側と復号化側とで暗号同期をとっていた。暗号同期とは、暗号化、復号化に用いる乱数を一致させて、暗号化したときと同じ乱数を復号化に用いるようにすることで、暗号同期をとることにより、暗号化されて伝送されてきたデータを確実にもとのデータに復号化できる。
【００１４】
【発明が解決しようとする課題】上記のように従来の暗号化方法は、暗号に使用する鍵が固定の値であった。そのため、第三者に鍵が渡ってしまった場合、第三者はその鍵を用いて容易に以後のすべて暗号文を解読すること

ができるという問題点があった。

【００１５】また、暗号化側と復号化側で暗号同期をとるために、乱数生成回路部に入力する初期値を１フレーム毎にある固定値にリセットしているので、乱数の周期は１フレームとなる。このように周期が短いと十分なランダム性が得られず、十分な暗号化強度（暗号の解きにくさ）を有しないという問題点があった。つまり、一フレームでリセットされるごとにまた同じ乱数を繰り返し用いることになるため、乱数に周期性があり、解読が比較的容易で、一度解読されると以降は同じ乱数により解読可能となってしまう。

【００１６】本発明は、上記問題点を解決するためになされたものであり、その目的は、より解読が困難でかつ暗号同期が確実にとれる暗号化装置および復号化装置、ならびに暗号化方法および復号化方法を提供することにある。

【００１７】

【課題を解決するための手段】上記目的を達成するために本発明の暗号化装置および復号化装置に係る発明の第一の構成は、基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムに係り、秘匿性を要する伝送データの暗号化に用いられる暗号化装置において、この暗号化装置は、暗号鍵を生成する暗号鍵生成部と、初期入力値を格納するレジスタと、暗号鍵生成部で生成した暗号鍵とレジスタに格納された初期入力値を入力し、予め定められた演算処理を行い乱数を生成し出力する乱数生成回路と、伝送データまたは暗号化データに対し、その乱数を用いて暗号化または復号化を施す演算部とを有し、暗号鍵生成部は、基地局と移動局との間の通信回線の接続ごとに設定される情報に基づいて暗号鍵を生成するようにしたものである。

【００１８】次に、第二の構成の暗号化装置および復号化装置は、上記第一の構成の暗号化装置および復号化装置において、鍵生成部は、通信回線の接続ごとに設定される情報として、基地局の基地局識別情報、移動局の移動局識別情報、基地局と移動局の通信接続情報、移動局の移動局認識情報、通信接続に関連する時間情報、移動局の位置情報等うちの一つまたは複数を用い、予め定められた演算規則に基づいて暗号化鍵を生成するようにしたものである。

【００１９】また、第三の構成の暗号化装置および復号化装置は、上記第一の構成の暗号化装置および復号化装置において、乱数生成回路は、予め定められた演算処理を行って生成した乱数列から、順々に乱数を生成する回路であって、ある乱数を生成して、その生成された乱数を入力値として乱数生成回路は次の乱数を生成し、その乱数を用いて演算部は伝送データまたは暗号化データに対し暗号化または復号化を施すようにしたものである。

【００２０】また、別に第四の構成の暗号化装置および復号化装置は、上記第一の構成の暗号化装置および復号化装置において、乱数生成回路に入力された初期入力値に予め定められた演算処理を施す初期値演算処理部をさらに有し、その演算処理を施した初期値をレジスタに格納し、その初期値を次の初期入力値として乱数生成回路は乱数を生成し、その乱数を用いて演算部は伝送データまたは暗号化データに対し暗号化または復号化を施すようにしたものである。

【００２１】また別に第五の構成の暗号化装置および復号化装置は、上記第一の構成の暗号化装置および復号化装置において、この通信システムによる通信は、フレームを伝送単位として行われ、そのフレームのフレーム番号をレジスタに格納し、そのレジスタに格納したフレーム番号を初期入力値として乱数生成回路は乱数を生成し、その乱数を用いて演算部は伝送データまたは暗号化データに対し暗号化または復号化を施すようにしたものである。

【００２２】また、上記目的を達成するために本発明の暗号化方法及び復号化方法に係る発明は、基地局と移動局との間の通信回線の接続ごとに設定される情報に基づいて暗号鍵を生成し、その暗号鍵と初期入力値を用いて、予め定められた演算処理を行い乱数を生成し、その乱数を用いて伝送データまたは暗号化データに対し暗号化または復号化を施すようにしたものである。

【００２３】より詳しくは、暗号鍵の生成は、通信回線の接続ごとに設定される情報として、基地局の基地局識別情報、移動局の移動局識別情報、基地局と移動局との通信接続情報、移動局の移動局認識情報、通信接続に関連する時間情報、移動局の位置情報のうちの一つまたは複数を用い、予め定められた演算規則に基づいて暗号化鍵を生成するようにしたものである。

【００２４】また詳しくは、乱数の生成は、予め定められた演算処理を行って生成した乱数列から順々に乱数を生成するものであって、ある乱数を生成して、その生成された乱数を入力値として、予め定められた演算処理を行い次の乱数を生成し、その乱数を用いて伝送データまたは暗号化データに暗号化または復号化を施すようにしたものである。

【００２５】また別に詳しくは、初期入力値に予め定められた演算処理を施し、その演算処理を施した初期値を再びまた次の初期入力値として乱数を生成し、その乱数を用いて伝送データまたは暗号化データに暗号化または復号化を施すようにしたものである。

【００２６】また別に詳しくは、この通信システムによる通信は、フレームを伝送単位として行われ、そのフレームのフレーム番号を初期入力値として乱数を生成し、その乱数を用いて伝送データまたは暗号化データに対し暗号化または復号化を施すようにしたものである。

【００２７】また、上記目的を達成するために本発明の通信システムに係る発明の第一の構成は、基地局と、その基地局と通信回線を介して通信を行う移動局を有する

通信システムにおいて、基地局および移動局は、上記第一の構成の暗号化装置および復号化装置を有するようにしたものである。

【００２８】また、本発明の通信システムに係る発明の第二の構成は、基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムにおいて、基地局および移動局は、上記第三の構成の暗号化装置および復号化装置を有するようにしたものである。

【００２９】また、本発明の通信システムに係る発明の第三の構成は、基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムにおいて、基地局および移動局は、上記第四の構成の暗号化装置および復号化装置を有するようにしたものである。

【００３０】また、本発明の通信システムに係る発明の第四の構成は、基地局と、その基地局と通信回線を介して通信を行う移動局を有する通信システムにおいて、基地局および移動局は、上記第五の構成の暗号化装置および復号化装置を有するようにしたものである。

【００３１】またより詳しくは、上記第二ないし第四の構成の通信システムにおいて、基地局と移動局との間のデータの伝送は制御情報領域と伝送情報領域を有する伝送スロットを介して行われ、基地局および移動局は、送信しようとする伝送スロットの制御情報領域が使用可能な状態であるかを判定する判定手段と、制御情報領域に暗号問期をとるための暗号問期情報を書き込む手段と、伝送スロットが暗号同期情報を伝送しているかどうかを示す暗号同期情報識別子を前記制御情報領域に付加する手段と、受信した伝送スロットの制御情報領域の暗号同期情報識別子から伝送スロットが暗号同期情報を伝送しているかどうかを判定する手段と、伝送スロットの制御情報領域から暗号同期情報を受け取る手段とをさらに有するようにしたものである。

【００３２】

【発明の実施の形態】以下、本発明に係る各実施形態を、図２ないし図１１を用いて説明しよう。

【００３３】各実施形態においては、暗号鍵、初期値、乱数、暗号文は、それぞれデータ長が６４ビットであるとし、データも６４ビット単位で暗号化および復号化処理を行うものとして説明する。しかしながら本発明は、データ長が６４ビットであることや、暗号鍵、初期値、乱数、暗号文の各値が同じデータ長である場合に特に限定されるものではない。

【００３４】〔実施形態１〕以下、本発明に係る第一の実施形態を、図２ないし図５を用いて説明する。

【００３５】図２（ａ）は、本発明の第一の実施形態における暗号化装置の構成とデータの流れを示した図である。

【００３６】図２（ｂ）は、本発明の第一の実施形態における復号化装置の構成とデータの流れを示した図である。

【００３７】図３は、本発明の暗号化装置の鍵の生成に用いる各種情報と、鍵生成部の構成を示す図である。

【００３８】図４（ａ）は、本発明の第一の実施形態における暗号化方法のフローチャートである。

【００３９】図４（ｂ）は、本発明の第一の実施形態における復号化方法のフローチャートである。

【００４０】本発明の暗号化装置および復号化装置は、図２に示すように、鍵生成部２００で生成した鍵を用いて、暗号化を行う。鍵生成部２００においては、基地局と移動局間で通信回線を接続する毎に設定される情報等に基づいて暗号鍵を生成する。鍵のもととなるこれらの情報は通信回線を接続する度に異なる値をとるものである。また、接続開始時間等の時間情報や、基地局が管理している移動局の位置情報は、通信接続中も時々刻々更新されている。従って、これらの情報から鍵を生成することにより、通信接続毎、もしくは特定または任意の時間毎に異なるダイナミックな値をとる暗号鍵とすることができる。

【００４１】また、本発明では暗号化開始時に、暗号化側と復号化側で予め決めておいたある初期値をレジスタ２０１に格納し、格納した初期値と暗号鍵を乱数生成回路部２０２に入力する。そして、なんらかの暗号化アルゴリズムに従って乱数を生成する。この暗号化アルゴリズムに関しては、例えばＩＳＯに登録されているものを用いることができる。この詳細については「日経エレクトロニクスＮｏ．６５８」の「インターネット時代の暗号技術」に詳しい。

【００４２】そして、生成した乱数と送信しようとするデータに排他的論理和演算部２０３で演算を施して暗号文を作成する。

【００４３】本発明においては、乱数生成回路部２０２から出力された乱数を、次の乱数生成のための初期値として、フィードバックして用いる。これにより、初期値を短い周期で固定の値にリセットする必要がなくなり、乱数生成器で生成する乱数に、十分なランダム性をもたせることができる。

【００４４】復号化側では、送信されてきた暗号文に対し、暗号化側と同様の手順により生成した乱数を用いて、排他的論理和演算を行い、データを復元する。

【００４５】鍵生成に用いる情報や、暗号化開始時に最初に乱数生成回路に入力する初期値は、暗号化側と復号化側で予め取り決めておく。または、鍵生成にどのような情報を用いているかについては、伝送データの制御情報領域に書き込んで送る方法も考えられる。これについては後で詳しく述べる。

【００４６】続いて、鍵生成部の動作について図３を用いて説明する。

【００４７】鍵生成部では、図３に示すような、基地局と移動局が共有する情報、あるいは通信接続毎に設定される情報のうちいずれかを組み合わせ、演算部３００に

おいて、あらかじめ定めておいた関数で演算を行い、暗号鍵を生成する。暗号鍵の生成に用いられる情報には、例えば基地局識別情報、移動局識別情報、通信接続情報、移動局認識情報、時間情報、位置情報がある。

【００４８】ここで、基地局識別情報は、各基地局を識別するために個々に割り当てられている情報である。移動局識別情報は、各移動局を識別するために個々に割り当てられている情報である。通信接続情報は、同一通信回線における接続上の識別を行うための情報である。移動局認識情報は移動局の認証を行うために使われる情報である。時間情報は、通信接続開始年月日・時刻情報や最終接続履歴年月日・時刻情報等である。位置情報は、移動局が在圏する位置を表す情報である。これらの情報は、主として通信接続時に設定されるものであるが、その他通信中に使用者の要求に基づいてキー操作により変更されたり、あるいは一定時間あるいはランダムな時間ごとに基地局と移動局が相互に伝送して共有するものである。

【００４９】以下に具体的な鍵の生成手順について説明する。

【００５０】ある通信システムにおいて、基地局識別情報は５６ビット、通信接続情報は１６ビットであらわされているとする。この基地局識別情報と、通信接続情報の下位８ビットから暗号鍵を生成する場合を例にとる。

【００５１】まず、基地局と移動局間で通信回線が接続され、基地局識別情報が３で、これは５６ビットで表現すると［００……１１］（…はすべて０、以下のビット表現においても同様）、通信接続情報が１５、これは１６ビットで表現すると［００……１１１１］と設定されたとする。これらを組み合わせて作成した６４ビットのデータは、［００……１１００００１１１１］となる。図３の３００の演算部が入力値をそのまま出力したとすると、この値が暗号鍵となる。

【００５２】次に、鍵生成部の演算部で行う演算について図４を用いて説明する。

【００５３】図４は、鍵生成部の演算部の一実施形態を示した図である。

【００５４】暗号鍵の解読をより困難にするためには、図４に示すような線形フィードバックシフトレジスタによる疑似乱数発生回路を演算処理に用いてもよい。フィードバックシフトレジスタによる疑似乱数発生回路については、岡本著「暗号理論入門」共立出版に詳しい。

【００５５】この図４において、Ｓｉ-1～Ｓｉ-nはレジスタである。ここでは暗号鍵のデータ長は６４ビットとして考えているので、ｎ＝６４である。

【００５６】演算の方法は、まずこのレジスタＳｉ-1～Ｓｉ-nに、基地局識別情報と通信接続情報を組み合わせて作成した６４ビットのデータ［００……１１００００１１１１］の各ビットの値を初期値として入力する。そして、各レジスタから値を読み出し（Ｃ1～Ｃn）、これを順次加算した値Ｓｉをｌビットずつ出力し、６４ビット単位で１つの暗号鍵とする。

【００５７】以上説明した暗号鍵を用いた暗号化および復号化手順を図５のフローチャートを用いて説明する。

【００５８】まず、図５（ａ）に示す暗号化方法は、通信回線を接続する毎に決まる情報や、時間情報、携帯端末、基地局の位置情報等に基づいて暗号化用の鍵を生成する（Ｓ５００）。次に、暗号化開始時に、乱数生成のための初期値を乱数生成関数に入力する（Ｓ５０１）。つづいて、入力された初期値とＳ５００で生成した暗号鍵を用い、暗号化アルゴリズムに基づいて演算を行って乱数を生成する（Ｓ５０２）。次に、暗号化するデータが入力されているかどうかの判定を行い（Ｓ５０３）、データが入力されていれば、データとＳ５０２で生成した乱数との排他的論理和演算を行い、暗号文を生成する（Ｓ５０４）。データが入力されていなければデータが入力されるまでＳ５０３の判定処理を繰り返す。Ｓ５０４で生成した暗号文を出力したあと、Ｓ５０２において生成した乱数を、次のデータの暗号化に用いる乱数を生成するための初期値として乱数生成関数に入力する（Ｓ５０５）。

【００５９】Ｓ５０２～Ｓ５０５の処理は、暗号化すべき全てのデータが暗号化されるまで繰り返し行う。

【００６０】次に、本発明の復号化装置による復号化方法は、図５（ｂ）に示すように暗号化方法と同様な手順で行われる。まず、暗号化側と同じ方法で通信接続毎に決まる情報や、時間情報、携帯端末、基地局の位置情報等から復号化用の鍵を生成し（Ｓ５１０）、暗号化開始時点では、暗号化側と予め決めておいたある初期値を乱数生成回路部に入力する（Ｓ５１１）。そしてその初期値と、Ｓ５１０で生成した暗号鍵から、なんらかの暗号化アルゴリズムに従って、乱数を生成する（Ｓ５１２）。次に、復号化すべき暗号文が入力されているかどうかの判定を行う（Ｓ５１３）。暗号文が入力されていれば、暗号文と乱数の排他的論理和演算を行ってデータを復元する（Ｓ５１４）。暗号文が入力されていなければ暗号文が入力されるまでＳ５１３の処理を繰り返す。Ｓ５１４で復号したデータを出力した後、Ｓ５１２で生成した乱数を、次のデータの復号化に用いる乱数を生成するための初期値としてＳ５１２の乱数生成関数に入力する（Ｓ５１５）。Ｓ５１２～Ｓ５１５の処理は、復号化すべき全ての暗号文が復号化されるまで繰り返し行う。

【００６１】［実施形態２］次に、本発明に係る第二の実施形態を、図６および図７を用いて説明する。

【００６２】図６（ａ）は、本発明の第二の実施形態における暗号化装置の構成図である。

【００６３】図６（ｂ）は、本発明の第二の実施形態における復号化装置の構成図である。

【００６４】図７（ａ）は、本発明の第二の実施形態における暗号化方法のフローチャートである。

【００６５】図７（ｂ）は、本発明の第二の実施形態における復号化方法のフローチャートである。

【００６６】本発明の第二の実施形態における暗号化装置においては、乱数生成回路に入力する初期値の設定が第一の実施形態と異なる。第二の実施形態では、第一の実施形態同様、初期値は暗号化開始時には暗号化側と復号化側で予め定めておいた値を用いる。しかし、その初期値にインクリメント、またはデクリメントなどの演算を施す処理部６０４を有し、以降はその処理後の値を乱数生成のための初期値として用いる。例えば、暗号化開始時の初期値が１であったとすると、これは６４ビットで表現すると［００……０１］となり、この初期値を１ずつインクリメントして次の初期値は２、６４ビットで表現すると［００……１０］、その次の初期値は３、６４ビット表現で［００……１１］と初期値が更新されていく。

【００６７】または、乱数生成のための初期値を、暗号化を施すデータのフレーム番号に基づいて設定することも考えられる。フレームとは送信データを数百ビットまとめた単位である。フレーム番号に基づいて初期値を設定することにより、１フレーム分のデータを暗号化するたびに定期的に初期値が更新されることになる。フレーム番号は、システムにもよるが例えば１５ビットで表される。本発明の各実施形態では初期値は６４ビットであるので、この１５ビットのフレーム番号を下位１５ビットとし、残りの４９ビットは０とするなどして６４ビットの初期値を得る。例えば、暗号化開始時に、データのフレーム番号が１１であったとすると、これに残りの４９ビットを０と設定して、初期値は［００……０１０１１］となる。１フレーム分のデータを暗号化するとき、フレーム番号は１２となり、次の初期値は６４ビット表現で［００……０１１００］）、その次の初期値は１３となり、これは６４ビット表現で［００……０１１０１］…と定期的に更新される。

【００６８】このように初期値を定期的に更新することにより、乱数生成回路で常に違う系列の乱数を生成することができ、暗号化強度が向上する。その他のブロックの処理内容は、第一の実施形態と同様である。

【００６９】復号化装置においても暗号化側と同様に、暗号化開始時は暗号化側と復号化側で予め定めておいた初期値を用いる。そしてその初期値にインクリメント、またはデクリメントなどの演算を施す処理部６１４を有し、以降はその処理後の値を乱数生成のための初期値として用いる。または、乱数生成のための初期値を、暗号化を施すデータのフレーム番号に基づいて設定する。その他のブロックの処理内容は、第一の実施形態と同様である。

【００７０】第二の実施形態においては、暗号鍵生成に用いる情報や、暗号化開始時に最初に乱数生成回路に入力する初期値、初期値に施すインクリメントまたはデクリメントなどの演算処理内容、またはフレーム番号から初期値を設定するかどうかといったことは、暗号化側と復号化側で予め取り決めておく。これらの暗号化側と復号化側で取り決める必要がある情報については、伝送するデータの制御情報領域に書き込んで送ってもよい。

【００７１】以下、図７を参照し、第一の実施形態と比較して本実施形態の暗号化方法および復号化方法を説明しよう。

【００７２】まず、暗号化方法は、ステップ７００～７０４までは第一の実施形態の暗号化方法のステップ５００～５０４と同様である。第二の実施形態においてはＳ７０４において暗号文を生成して出力したあと、乱数生成回路への前回の初期値入力にインクリメントまたはデクリメントなどの演算処理を施して、次の乱数生成のための初期値として乱数生成関数に入力する（Ｓ７０５）。あるいはフレーム番号に基づいた値を初期値として設定し、乱数生成関数に入力する。

【００７３】復号化方法も、Ｓ７１０～７１４までは第一の実施形態の復号化方法のＳ５１０～５１４と同様である。第二の実施形態においてはＳ７１４において復元したデータを出力したあと、乱数生成回路への前回の初期値入力にインクリメントまたはデクリメントなどの演算処理を施して、次の乱数生成のための初期値として乱数生成関数に入力する（Ｓ７１５）。あるいはフレーム番号に基づいた値を初期値として設定し、乱数生成関数に入力する。

【００７４】［暗号同期］次に、暗号化装置と復号化装置の暗号同期について説明する。

【００７５】暗号同期とは、暗号化、復号化に用いる乱数を一致させて、暗号化したときと同じ乱数を復号化に用いるようにすることで、暗号同期をとることにより、暗号化されて伝送されてきたデータを確実にもとのデータに復号化できる。

【００７６】以上の第一および第二の実施例で説明した本願発明の暗号化装置および復号化装置、ならびに暗号化方法および復号化方法によれば、乱数生成回路に入力する初期値が１フレーム毎にリセットされて同じ値が入力されず、同じ乱数が発生するということがないので、暗号用乱数の周期を必要なだけ長くできる。このように暗号に用いる乱数の周期を長くすると、第３者による暗号解読が困難になり、暗号化強度を増すことができる。

【００７７】しかし、その反面、携帯電話での通信中にチャネルが切り替わったときや、物陰に移動局が隠れ一時的に通話ができなくなったときに暗号化側と復号化側の暗号化のための暗号化鍵や乱数が一致しなくなり、稀に暗号化装置と復号化装置の暗号同期がとれなくなる恐れがある。

【００７８】つまり、通信中チャネルが切り替わったり、物陰に移動局が隠れて一時的に通話ができなくなった場合、しばらくのあいだ受信側は送信側から送られて

くる暗号文を受け取れなくなる。その後通話が回復すると、受信側は再び暗号文を受け取るが、その暗号文は通話回復後の暗号鍵および乱数を用いて暗号化されたものである。一方受信側においては復号化に用いる暗号鍵と乱数は通話回復前のものであるため、送られてきたデータを復元できなくなる。従来の暗号化では、１フレームごとに初期値をリセットすることにより、暗号化の強度が弱まるかわりに、そのような場合にも１フレームの間に暗号化側と復号化側で暗号鍵および乱数を再び同じにして暗号同期を確保していた。

【００７９】本発明においては、第一および第二の実施例で述べた暗号化装置および復号化装置ならびに暗号化方法および復号化方法に加え、暗号化側と復号化側の暗号同期外れを防止するために、以下のような暗号同期方法および通信スロットのフォーマットを提供する。つまり、通信スロットに、暗号同期をとるための暗号同期情報を書き込み、暗号化データとともに伝送する。

【００８０】図８は、暗号同期情報を書き込んだ本発明の伝送スロットの例である。

【００８１】一般的に、暗号通信に用られている通信用スロットにおいては、制御情報領域は、通信接続中ほとんど使用されていない。本発明では、この通信スロットの制御情報領域が使用されていない時に、乱数生成回路に入力する初期値等、暗号化のための乱数を生成するのに必要な値を制御情報領域を使って、暗号文と一緒に伝送することにより暗号同期外れを防止する。例えば、第二の実施形態においては、初期入力値として用いているフレーム番号を、この領域に書き込んで伝送する。

【００８２】通信スロットの制御情報領域が１６ビットであるシステムでは、このうち１ビットを暗号同期情報を伝送していることを示す識別子として用いる。そしてこの識別子を暗号同期情報を伝送しているときは１、伝送していないときは０に設定する。そして残りの１５ビットで第二の実施形態でも述べた１５ビットのフレーム番号を伝送する。例えば、フレーム番号１２を暗号同期情報として伝送する場合には、制御情報領域は先頭１ビットを識別子として１を設定し、［１００……０１１００］（１６ビット）となる。復号化側では、送られてきた伝送スロットの制御情報領域に書き込まれたフレーム番号をもとに暗号化側と同じ乱数を生成し、暗号化データを確実に復号化することができる。

【００８３】また、暗号同期情報の送信手順を図９を用いて説明する。

【００８４】図９は、暗号同期情報の送信手順を示すフローチャートである。

【００８５】まず、制御情報領域が使用可能な状態であるか判定を行う（Ｓ９００）。もし、使用可能な状態であれば、暗号同期情報を伝送していることを示す識別子を付ける（Ｓ９０１）。使用不可能な状態であれば暗号情報は伝送しない（Ｓ９０４）。Ｓ９０１で識別子を付けた後、暗号識別情報を制御情報領域に入力する（Ｓ９０２）。そして、暗号同期情報を制御情報領域に入力した通信スロットを伝送する（Ｓ９０３）。

【００８６】次に、暗号同期情報の受信手順を図１０を用いて説明する。

【００８７】図１０は、暗号同期情報の受信手順を示すフローチャートである。

【００８８】まず、制御情報領域の識別子から、受信した伝送スロットが制御情報領域を利用して暗号同期情報を伝送しているかどうか判定する（Ｓ１０００）。暗号同期情報を伝送していない場合は、制御情報領域から暗号同期情報を受け取らない（Ｓ１００２）。暗号同期情報を伝送している場合は、制御情報領域から暗号同期情報を受け取る（Ｓ１００１）。

【００８９】以上の処理によって、制御情報領域が使用可能なときに暗号同期情報を送受信し、暗号化と復号化の間の暗号同期をとることができる。

【００９０】次に、情報チャネルへの暗号同期情報の割り当てについて図１１を用いて説明する。

【００９１】図１１は、暗号同期情報の情報チャネルへの割り当て例を示す図である。

【００９２】通常の音声情報の伝送ビットレートが、１１．２Kbit/secである場合を例にとって説明する。図１１に示すように、音声情報のビットレートを１１．２Kbit/secから８Kbit/secにすると、残りの３．２Kbit/secを使って暗号同期情報を伝送することができる。さらに、音声情報のビットレートを５．６Kbit/secにすると、残りの半分の帯域である５．６Kbit/secを使って暗号同期情報を伝送することができる。さらに、音声情報のビットレートを４Kbit/secにすれば、残りの７．２Kbit/secを用いて暗号同期情報を送ることができる。

【００９３】また、以上の暗号同期方法は、移動電話の場合を想定して説明したが、モデム等を接続してデータ通信を行う際も同様に、制御情報領域一つの通信スロット内の通信データの割合を減らすことによって生じたビットを使い、暗号制御情報を送ればよい。以上の処理によって、フレーム毎に乱数もしくはフレーム番号を伝送でき、暗号化と復号化の間の暗号の同期をとることができる。以上のように暗号同期を獲得できることでより安定した暗号化通信が可能となる。

【００９４】

【発明の効果】本発明によれば、従来より、より解読が困難でかつ暗号同期が確実にとれる暗号化装置および復号化装置、ならびに暗号化方法および復号化方法を提供することができる。

【００９５】また、暗号化側と復号化側の暗号同期がとれ安定した通信が確保できる暗号化装置および復号化装置、ならびに暗号化方法および復号化方法を提供することができる。

【図面の簡単な説明】

【図１】暗号化装置および復号化装置を利用した携帯電話システム全体の構成図である。

【図２】（ａ）本発明の第一の実施形態における暗号化装置の構成とデータの流れを示した図である。

（ｂ）本発明の第一の実施形態における復号化装置の構成とデータの流れを示した図である。

【図３】本発明の暗号化装置の鍵の生成に用いる各種情報と、鍵生成部の構成を示す図である。

【図４】鍵生成部の演算部の１実施形態を示した図である。

【図５】（ａ）本発明の第一の実施形態における暗号化方法のフローチャートである。

（ｂ）本発明の第一の実施形態における復号化方法のフローチャートである。

【図６】（ａ）本発明の第二の実施形態における暗号化装置の構成およびデータの流れを示す図である。

（ｂ）本発明の第二の実施形態における復号化装置の構成およびデータの流れを示す図である。

【図７】（ａ）本発明の第二の実施形態における暗号化方法のフローチャートである。

（ｂ）本発明の第二の実施形態における復号化方法のフローチャートである。

【図８】暗号同期情報を書き込んだ本発明の伝送スロットの例である。

【図９】暗号同期情報の送信手順を示すフローチャートである。

【図１０】暗号同期情報の受信手順を示すフローチャートである。

【図１１】暗号同期情報の情報チャネルへの割り当て例を示す図である。

【図１２】（ａ）従来の通信システムに用いられている暗号化装置の構成と、データの流れを示した図である。

（ｂ）従来の通信システムに用いられている復号化装置の構成と、データの流れを示した図である。

【符号の説明】

１００，１０１，１０２…移動体端末、１０３，１０４，１０５…基地局、１０６…交換制御局、１０７…固定電話網、１０８…電話機、１０９…暗号化／復号化装置、２００，２１０…鍵生成部、２０１，２１１…レジスタ、２０２，２１２…乱数生成回路部、２０３，２１３…排他的論理和演算部、３００…演算部、６０４，６１４…初期値演算処理部、１２００，１２１０…ＰＮパターン発生回路、１２０１，１２１１…排他的論理和演算部。

【図１】

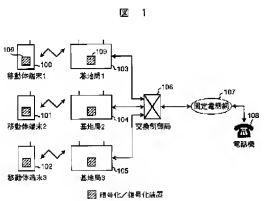
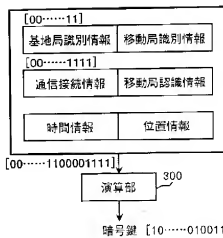


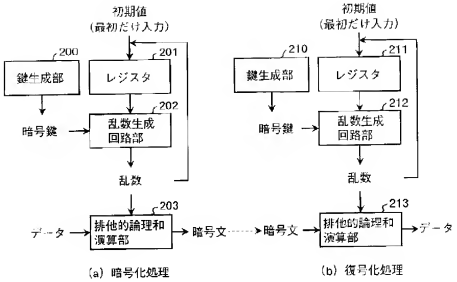
図 暗号化／復号化装置

【図３】



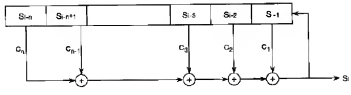
【図２】

図　2



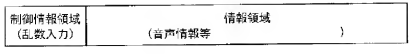
【図４】

図　4



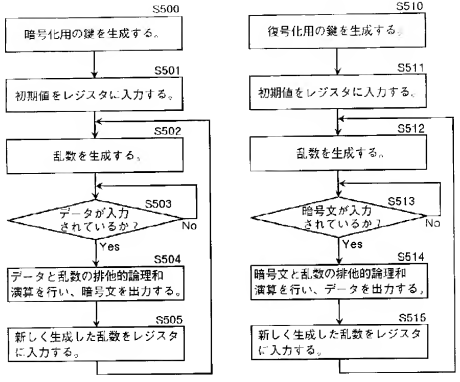
【図８】

図　8



【図５】

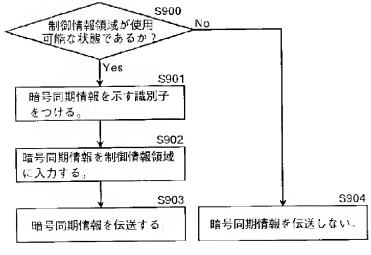
図　５



(a) 暗号化処理　　(b) 復号化処理

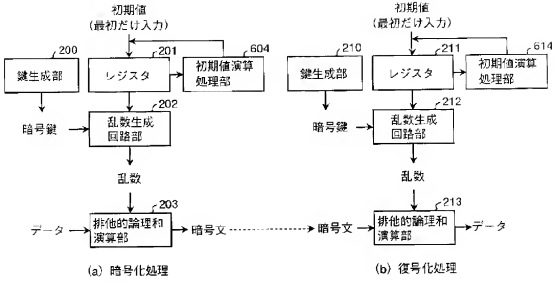
【図９】

図　９



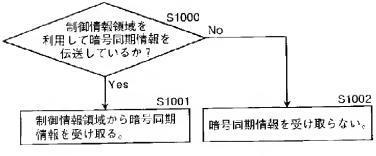
【図６】

図　6


初期値
(最初だけ入力)
200
鍵生成部
201
レジスタ
604
初期値演算処理部
暗号鍵
202
乱数生成回路部
乱数
203
データ
排他的論理和演算部
暗号文
(a) 暗号化処理
初期値
(最初だけ入力)
210
鍵生成部
211
レジスタ
614
初期値演算処理部
暗号鍵
212
乱数生成回路部
乱数
213
暗号文
排他的論理和演算部
データ
(b) 復号化処理

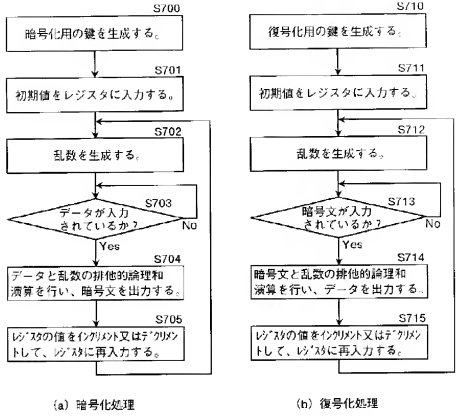
【図１０】

図　1 0


S1000
制御情報領域を利用して暗号同期情報を伝送しているか？
No
Yes
S1001
制御情報領域から暗号同期情報を受け取る。
S1002
暗号同期情報を受け取らない。

【図７】

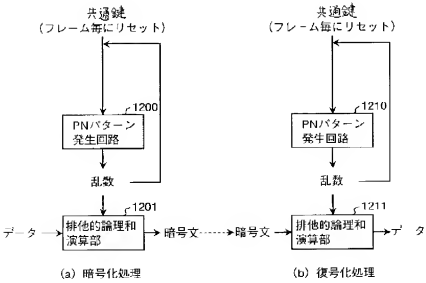
図　７



(a) 暗号化処理　　(b) 復号化処理

【図１２】

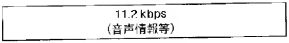
図　１２



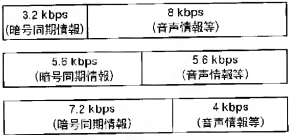
(a) 暗号化処理　　(b) 復号化処理

【図１１】

図　１１



（ａ）従来の情報チャンネル



（ｂ）本発明の情報チャンネル